IMPLEMENTATION OF TARGETED FINANCIAL SANCTIONS AND CONTROLS AGAINST PROLIFERATION FINANCING

Guidance Note 2 of 2021 for Non-Bank Financial Institutions

Updated January 2021

Disclaimer

This Guidance Note is authored by the NBFIRA in line with section 44(1)b of the Financial Intelligence Act and Regulations 2019 ("FI Legislation") of the Republic of Botswana for comprehensive use by the NBFIs. The note is indicative and while due care was exercised to ensure that this guideline is accurate and consistent with the FI Legislation, the latter shall prevail in the unfortunate case of ambiguity and NBFIRA does not guarantee or take any liability whatsoever.

Table of Contents

1. **Introduction**

1.1 This guidance is in line with Financial Action Task Force ("FATF") Recommendations[1] 1 & 7 and issued in accordance with section 44 (1) (b) of the Financial Intelligence Act of 2019.

1.2 Recommendation 1 requires Non-Bank Financial Institutions (NBFIs) amongst other Designated Non-Financial Businesses and Professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering, terrorism financing and proliferation financing risks.

1.3 Recommendation 7 states that countries are required to implement targeted financial sanctions imposed under United Nations Security Council Resolutions related to the proliferation of Weapons of Mass Destruction ("WMDs") and the financing of proliferation. Implementation of these resolutions requires countries to freeze without delay:

(a) All funds or other assets that are owned or controlled by the designated person or entity, not just those that can be tied to a particular act, plot or threat of proliferation;

(b) All funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities;

(c) Funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities; and

(d) Funds or other assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities.

1.4 Recommendation 7 further emphasizes the need for firms to implement preventive measures to counter the flow of funds or assets to proliferators or those who are responsible for weapons' proliferation.

2. **Scope**

2.1 The following guidance should be read within the framework and provisions of:

a) Financial Intelligence Act, 2019 and its Regulations, 2019

b) Counter Terrorism Act 2014, and (Amendment Act 2018)

c) Counter-Terrorism Implementation of United Nations Security Council Resolutions) Regulations, 2020

d) Nuclear Weapons (Prohibition) Act, 2018

e) Biological Weapons (Prohibition) Act, 2018

f) Chemical Weapons (Prohibition) Act, 2018

g) Chemical, Biological, Nuclear and Radiological Weapons Management Authority, established under the Chemical Weapons Prohibition Act, 2018

h) Other guidance papers issued by the Regulatory Authority from time to time;

[1] As updated in October 2020

i) FATF Recommendations

j) FATF Guidance on Counter Proliferation Financing ("CPF"): The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction[2];

k) FATF's publication "Combating Proliferation Financing: A status report on policy development and consultation"[3];

l) FATF Proliferation Financing Report[4];

3. Purpose

3.1 This guidance is issued to raise awareness of proliferation financing threats, vulnerabilities and risks thereof; and to highlight the relevant requirements for NBFIs.

3.2 Any NBFI that plays a role in PF, either knowingly or unknowingly, would cause immense damage to itself, and to the security and integrity of the financial system. The identification, assessment, understanding, and management of PF risks by NBFIs is essential to a robust AML/CFT regime. It is critical that every firm includes CPF in its AML/CFT programme and risk management strategies.

3.3 This guidance provides common definitions surrounding PF and describes the regulatory framework in Botswana, coupled with international standards and obligations.

3.4 This guidance also focuses on indicators of possible PF risks, and the relevant risk management practices and tools firms should implement and incorporate in their AML/CFT programmes to counter the ~~risks~~ threats and vulnerabilities associated with PF.

4. Definitions

Proliferation

4.1 FATF's 2008 Typologies and Proliferation Financing Report's definition of "Proliferation" is: "Proliferation has many guises but ultimately involves the transfer and export of technology, goods, software, services or expertise that could be used in nuclear, chemical or biological weapon-related programmes, including delivery systems; it poses a significant threat to global security."

Proliferation Financing

4.2 The 2010 FATF Status Report on Combating Proliferation Financing defines PF as: "the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations".

[2] issued in February 2018
[3] issued in February 2010
[4] issued in June 2008

Proliferation Financing Risk

Proliferation financing risks refers to the potential breach, non-implementation or evasion of the targeted financial sanctions obligations referred to in Recommendation 7.

Proliferator

4.3 The 2010 FATF Status Report on Combating Proliferation Financing defines proliferator as an individual or group of individuals that abuse both the formal and informal sectors of the international financial system or resort to cash in order to trade in proliferated goods.

Account

4.4 The term "account" should be construed as also meaning policy, mandate, matter, instruction, or engagement.

5. General framework for managing CPF

5.1 NBFIs must include CPF in their AML/CFT programme and risk management strategies, including in their Institutional Risk Assessment ("IRA");

5.2 NBFIs must effectively mitigate PF risk through application of their general AML/CFT programme and measures, including through monitoring for and reporting suspicious transactions;

5.3 NBFIs must conduct enhanced due diligence ("EDD") when dealing with:

(a) countries that are subject to UN sanctions or other high-risk countries identified by FATF;

(b) entities established in, or having a significant presence in, those countries; or

(c) transactions associated with those countries;

5.4 NBFIs that choose to do business in or involving countries that are high-risk for PF (as identified in the National Risk Assessment ("NRA") of ML, TF and PF, by supervisors, or by the NBF's own risk assessment), or accept customers with substantial ties to such countries, must:

(a) perform EDD on any transaction involving any such country;

(b) perform EDD on all customers with substantial ties to such countries and any transactions conducted by such countries.

EDD must be designed to ensure that the NBFI understands and manages the PF risk of the relationship.

5.5 NBFIs must be sensitive to the risks of transactions involving nuclear, dual-use, or military goods. NBFIs must perform EDD on:

(a) all customers with substantial ties to these goods or sectors; and

(b) all transactions involving these goods or sectors.

6. Proliferation Threats

6.1 PF threats are primarily external and relate to foreign state and non-state actors attempting to exploit banks, companies, or transportation infrastructure to clandestinely finance, procure, ship, or trans-ship goods for use in the proliferation of WMD. Traditionally, the most active PF threats have been states seeking to obtain or expand capabilities related to nuclear weapons and other WMD, although non-state actors also pose proliferation and PF threats. The current priority threats are:

(a) **State actors - l**i**sted countries** have created global networks of front and shell companies and employ complex, deceptive methods to conceal their proliferation finance activity and evade international sanctions levied against them. Other states with existing or developing WMD capabilities pose a more limited threat.

(b) **Non-state actors - terrorist groups** that have targeted countries for fundraising have at least stated an intent to pursue nuclear weapons and radiological materials.

6.2 NBFIs should be aware, however, that the absence of direct links to these countries or non-state actors does not mean that a transaction or customer is necessarily low risk. Proliferators have shown a high level of ability to hide their involvement and the nature of the activity underlying a transaction or business relationship. Every NBFI faces a certain amount of risk and must remain vigilant in protecting against proliferation and PF.

7. Vulnerabilities to PF

7.1 Examples of factors specific to PF that raise the level of risk are:

(a) Licit commercial and financial links with high-risk jurisdictions;

(b) Weaknesses in shipping and transhipment controls, including transparency, monitoring capabilities or any other discrepancies in the trade finance requirements;

(c) Insufficient familiarity with the list of dual-use goods for monitoring; and

(d) Insufficient understanding, awareness, and expertise of PF risks.

Common PF vulnerabilities

7.2 Proliferators in high-risk jurisdictions know that sanctions filters and due diligence procedures used by firms will detect and freeze transactions involving their true names. Instead, these actors employ a variety of tactics to evade detection and gain access to the international financial system. Examples of such tactics include:

(a) **Disguising themselves as residents of another jurisdiction.** Proliferators will structure transactions or corporate actions in order to appear to be a legitimate business based in a lower-risk jurisdiction, often one neighbouring the sanctioned country. Shell and front companies and firms in some countries have been implicated in recent sanctions evasions schemes directed from the UN listed countries; and

(b) **Use of opaque shell and front companies and complex corporate forms.** Proliferators use shell and front companies, particularly those established in jurisdictions with weak company formation regimes, to disguise their identities. These bad actors may use multiple complex layers of companies to further disguise ownership.

Proliferators may use both strategies at the same time to increase their chances of success.

8. Incorporating PF risk in the NBFI risk assessment

8.1 NBFIs must adopt a risk-based approach to managing their PF risks, as with ML and TF risks. The first step in adopting a risk-based approach is understanding PF risk, including by conducting an assessment of the overall PF risk in the NBFI operations. This assessment should be conducted as part of the NBFI institutional risk assessment (IRA).

8.2 The IRA must consider the following PF risks that an NBFI can be exposed to, directly or indirectly:

(a) **Customers** - the nature of customers;

(b) **Products and services** - the nature of the products and services offered to customers;

(c) **Delivery channels** - the means employed to deliver products and services to customers; and

(d) **Jurisdictions** - the countries or geographic regions in which the firm does business or where the customer is located or operates.

8.3 Each of these risk factors is addressed below.

8.3.1 Customer risk

There are several sources of PF risk from customers:

(a) Designated names - NBFIs are prohibited from offering financial services to UN-designated individuals and entities;

(b) Individuals and entities owned or controlled by designated names:

(i) Even if NBFIs are legally allowed to accept as a customer a company that is partly owned by a sanctioned person, they must be aware that such a company may also be involved in proliferation activity and poses elevated risks;

(ii) Sanctioned individuals may also seek to obscure their interest through family members or close business associates;

(iii) In the case of higher-risk companies, NBFIs should consider lowering the 20 percent ownership and control threshold to verify the identity of additional beneficial owners;

(iv) Applying the RBA, NBFIs should decide whether they are willing to accept customers in which a designated person has a non-controlling ownership interest; and

(c) Legitimate customers in industries that produce sensitive goods, dual-use goods, or companies or institutions involved in advanced research can pose PF risk to an NBFI:

(i) Shipping companies, particularly those serving high-risk regions, may also present risks;

(ii) Customers who produce dual-use goods may not be familiar with the rules and regulations governing exports. Customers that are unaware of the need to implement their own PF safeguards present higher risk to NBFIs; and

(iii) Proliferation networks often rely on shell and front companies to disguise end-users and payments. These companies are high-risk for a number of reasons, including their potential roles in PF typologies.

Product and service risk

8.3.2 Elevated PF risks related to products and services offered by NBFIs include:

(a) Trade finance transactions that involve controlled goods or technology-

(i) The complexity of these transactions can allow individuals and entities to hide their intentions or underlying illicit activities; and

(ii) Both traditional document-based trade finance transactions and cross-border wires related to trade present high PF risk to NBFIs.

(b) Cross-border wires involve greater PF risk than traditional trade finance and are often more attractive to bad actors:

(i) Wire transfers often include less information on the underlying activity, making it more difficult for NBFIs to fully understand the transaction;

(ii) NBFIs might find it difficult to obtain information on and understand the activity underlying cross-border wire transfers;

(iii) Wire transfers also provide a less complicated means for conducting trade transactions because they can be processed more easily than traditional trade finance instruments such as letters of credit, which usually involves extensive documentation and diligence.

(c) Correspondent banking services are another important source of PF concern:

(i) Activities such as clearing intermediary wires expose the NBFIs to additional risk because the institution must process or execute transactions for the customers of the firm's customer; and

(ii) The risk is elevated when the correspondent relationship exposes an NBFI to a region with links to proliferation activity.

Delivery channel risk

8.3.3 NBFIs should assess the risks associated with the delivery channels and apply special attention and EDD to the identified high-risk areas as per their risk-based approach. NBFIs should consider the channels used to take on new clients, as well as how those clients are accessing the products and services. Special attention should be paid to the channels that are not normally used by customers or are not line with normal behavioural pattern of the customer.

Jurisdiction risk

8.3.4.1 Countries that are known or strongly suspected to be developing WMD present the highest jurisdiction risk for NBFIs. The United Nations Security Council (UNSC) identifies the Democratic People's Republic of Korea (DPRK) and Iran as the main sources of PF threat globally.. These countries are top priorities in global counter-proliferation efforts because of their longstanding WMD programmes.

8.3.4.2 Proliferation risk, however, is not solely tied to countries at high-risk for proliferation or PF. Countries and terrorist groups rely on transnational connections to procure illicit goods and services.

Proliferators may aim procurement efforts at countries with weak export control laws, and they may choose to have sensitive or dual-use items delivered initially to transhipment hubs rather than directly to their home countries.

9. Implementation of preventive measures

9.1 NBFIs must ensure that their comprehensive AML/CFT programme – as well as their group-wide AML/CFT programme – is designed to manage PF risks identified in the institutional risk assessment effectively. AML/CFT policies and procedures must cover PF and reflect counter-PF guidance and warnings issued by the NBFIRA and the FATF.

9.2 NBFIs are required to:

(a) Offer relevant staff training on all AML/CFT risks as well as PF risks and red flags;

(b) Design and implement transaction monitoring systems to identify transactions that may be linked to PF; and

(c) Include potential PF-related activity in their transaction reporting and monitoring system.

Enhanced Due Diligence

9.3 NBFIs must conduct EDD on all customers and transactions that are assessed to be high risk for PF. EDD is a crucial preventive measure, that, when properly conducted, can help firms manage their PF risk.

9.4 EDD should focus on obtaining information regarding expected customer behaviour, with special attention to the expected end-users of any sensitive products and the customer's expected exposure to high-risk jurisdictions, including transhipment hubs. Customers in this group should also be monitored carefully, since unusual behaviour, even if not clearly suspicious, is more concerning in the case of customers that may potentially be exploited by proliferators.

9.5 NBFIs should also apply EDD to transactions found to involve any proliferation-sensitive goods or services, regardless of whether the firm's customer is itself in a high-risk category. As with onboarding, special attention should be paid to identifying the end-users of any sensitive goods.

9.6 Examples of EDD measures include, but are not limited to:

(a) Identifying beneficial owners below the 20 per cent threshold;

(b) Requiring the customer to sign a warrant or other agreement that it complies with all UN and Botswana sanctions;

(c) Requiring customers to submit a list of important suppliers and customers, and conducting basic due diligence and public records searches on these entities;

(d) Reviewing the customer's customer acceptance policy, sanctions policy, and any policies related to export controls, and requiring the customer to make changes if these policies are not sufficient;

(e) Subjecting the account to special transaction monitoring rules designed to raise alerts about new counterparties or other changes; and

(f) Reviewing the customer's transactions on the account on a more frequent basis to identify irregular transactions, changes in the customer's behaviour, or new counterparties.

9.7 In addition, NBFIs should consider applying enhanced measures for individual transactions, such as asking the customer to provide a valid export license or a reference to the export control requirements in the relevant jurisdiction showing that the exported goods do not require a permit.

10. Implementation of Targeted Financial Sanctions

Customer Screening

10.1 NBFIs are required to screen the entire customer file for all customers, including beneficial owners, authorised signatories, and addresses, whenever a new designation is announced. For customers being onboarded, all such customers should be screened before onboarding. If no customer relationship is formed (*e.g.*, the customer is a walk-in or wants to engage in a one-time transaction), customers must be screened before making a transaction.

10.2 It is not sufficient for an NBFI to simply screen its customer lists against the names of sanctioned individuals or entities. To ensure that they are complying with the requirement to freeze all funds that the designated person controls, even indirectly, NBFIs must conduct appropriate due diligence to satisfy themselves that they know who their customers are and, if their customers are controlled by a third party, who that individual or entity is.

Example: *Company A is a customer of a BC firm. To identify whether Company A's accounts must be frozen, the firm must screen not just the name of Company A, but the names of its beneficial owner(s), anyone identified as having operational control of the company including persons holding a Power of Attorney, all signatories on the account, and all addresses provided by Company A during the CDD process (or available through a public records search).*

10.3 In addition, NBFIs must maintain real-time sanctions screening systems in place for all incoming and outgoing payments. These systems must be capable of identifying a match against any internal and vendor-supplied lists maintained by the NBFI, and if there is a match, holding the transaction until an appropriate employee of the NBFI reviews it.

10.4 Screening lists used in transaction monitoring must be updated immediately upon notice of designation. Where the NBFI uses a screening list provided by a third-party vendor, the vendor's Service Level Agreement with the NBFI must ensure that the screening list is updated within 2 hours of a new or updated designation being issued. Transaction screening and monitoring systems should be capable of screening and monitoring all aspects of customer onboarding as well as payment messages, including all additional information provided by the ordering institution or the customer. NBFIs **are strongly urged to include relevant terms, such as common types of dual-use goods, jurisdictions subject to sanctions, and major cities and ports within those jurisdictions, on their sanctions screening lists**.

Freezing accounts

10.5 Implementing targeted financial sanctions requires firms to place a restriction on any account meeting the following criteria.

(a) The account represents funds or other assets that are owned or controlled by the designated person or entity, beyond those that can be tied to a particular act, plot or threat of proliferation.

(b) The account represents funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities.

(c) The account represents funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities.

(d) The account represents funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities.

Holding/stopping transactions

10.6 Firms must screen all outgoing and incoming transfers in real-time and monitor transactions to detect any transactions that must be stopped or take any further actions. If a customer of an NBFI seeks to make a transfer or carry out a transaction to an individual or entity subject to UN or Botswana sanctions, the NBFI should immediately if the match is identified:

(a) hold the funds that would have been subject to the transfer and/or transaction;

(b) file an STR;

10.7 The funds should not be returned to the customer and should remain with the NBFI until the competent authorities have carried out a full investigation into the purpose of the payment and the nature of the customer's relationship with the designated person. NBFIs should comply with the directions of the competent authorities regarding ultimate disposition of the funds. NBFIs should in no case provide the customer with any information indicating that an STR has been filed.

Reporting

10.8 NBFIs are required to immediately and within at most 8 hours of implementing the designation order, to report any actions taken in compliance with the designation to the National Counter Terrorism Committee (NCTC) within 8 hours of compliance with the designation order, including submitting a Nil return to the NCTC:

(a) any accounts frozen;

(b) any transactions carried out, stopped, held or blocked related to the funds and assets;

(c) all screening performed; and

(d) any other efforts to comply with sanctions.

10.9 NBFIs are also required to immediately and within 5 days, to report to the FIA, a Suspicious Transaction Report (STR) related to the identified and frozen funds and assets. The STR must however be filed with the FIA within 48 hours where it involves wire transfers into and out of Botswana.

10.10 NBFIs must send acknowledgement of receipt of designation list to the NBFIRA within 7 days.

10.11 Once the above reports have been made, NBFIs are required to report any additional steps taken with respect to the identified funds or assets including when they freeze any additional accounts or funds or block any transactions. Account and /or customer relationship should be subject to enhanced monitoring as well.

False positives

10.11 List-based screening may result in hits where a person related to an account or transaction has the same name or the same address as a designated person. NBFIs are required to take a conservative approach to sanctions hits; that is, they cannot assume that a hit is a false positive and must thoroughly investigate every hit.

10.12 Generally, in such an investigation, NBFIs should compare information that is known about the party in question, such as date of birth and address, with other information provided in the designation order. If the party in question is not a customer, the NBFI may need to request that its customer provide reliable proof of its counterpart's identity, such as a copy of a government-issued photo identification document. If the NBFIs identifies information that establishes that the party in question is not a designated person, then the NBFI does not need to block a transaction or hold an account. Detailed records should be kept of the process followed, the evidence obtained, and the rationale for releasing a transaction.

10.13 **To avoid duplicative investigations, NBFIs may create a "false hit list / white list" and records of customers that have the same name as designated persons and whom the firm has determined, after a thorough investigation, not to be the person that has been designated**. NBFIs can use this list to instruct their automated monitoring software not to alert on such matches. While this practice is acceptable, it does carry risk, and therefore NBFIs should regularly review and update the list to ensure that bona fide matches are not suppressed. NBFIs would be well-advised also to subject the list to independent or external audit periodically.

10.14 NBFIs may also be approached by persons who claim that their funds or accounts have been mistakenly frozen because they share the same name as a designated person. Where property or other economic resources were frozen as a result of similarity in names or wrong entries on the United Nations list or national list or in the account of a person or entity being investigated, or as a result of any other error, the person affected may apply to the Minister to unfreeze the property or economic resources.

Unfreezing

10.15 Unfreezing will generally take place when a formerly designated person is no longer designated. De-listing may occur through publication of the Minister's Notice in the Gazzette or local newspaper or upon a court order.

10.16 Although rare, designations may be rescinded. For example, a designated person may cease to be involved in proliferation activities and therefore be removed from UN and Botswana sanctions list. A designated individual can also be removed from the sanctions lists after that individual's death upon request from court or from the heirs.

10.17 NBFIs may also receive court orders, or orders from the Minister to unfreeze funds and accounts for certain purposes, including, for example, to reflect the rights of third parties. NBFIs should seek guidance from the NCTC, FIA and NBFIRA if they have any questions about compliance with such orders.

10.18 NBFIs must continue to monitor updates to the Botswana sanctions list so that they are aware that a person has been de-listed. Unfreezing should take place promptly and within 8 hours but with appropriate due diligence and deliberate caution, consistent with the terms of de-listing and any guidance from authorities. NBFIs must continue to be vigilant to ensure that accounts or funds are not transferred to other designated persons. NBFIs that have questions about unfreezing the assets of a person that has been de-listed should seek guidance from the National Counter-Terrorism Committee (NCTC), FIA and NBFIRA.

Penalties

10.19 The Counter-terrorism laws sets strict penalties for failure to comply with the legal requirements, including the freezing of funds, that results from domestic or UN designations. Any person contravening a designation order can be sentenced to imprisonment and to a fine or both penalties. There is no requirement that a person knew that they were contravening the designation order, or that the person intended to contravene the order. Since freezing of accounts or transactions is a consequence of a designation order, failure to comply with these requirements can lead to extremely high fines and even a prison term. Each violation could be penalised separately.

11. **Red flag indicators and typologies of potential PF risks**

The below red flags and typologies are intended to assist NBFIs to identify potential proliferators, suspicious transactions and behavior patterns that are indicative of proliferation financing.

11.1 Customer:

(a) The customer is involved in the supply, sale, delivery or purchase of dual-use, proliferation-sensitive or military goods, particularly to higher risk jurisdictions.

(b) The customer or counterparty, or its address, is the same or similar to that of an individual or entity found on publicly available sanctions lists.

(c) The customer is a military or research body connected with a higher risk jurisdiction of proliferation concern.

(d) The customer's activities do not match the business profile.

(e) The customer is vague about the end-user(s) and provides incomplete information or is resistant when requested to provide additional information.

(f) A new customer requests a letter of credit from an NBFI, while still awaiting approval of its account.

(g) The customer uses complicated structures to conceal involvement, for example, uses layered letters of credit, front companies, intermediaries and brokers.

11.2 Transactions/Orders:

(a) The transaction(s) concern(s) dual-use, proliferation-sensitive or military goods, whether licensed or not.

(b) The transaction(s) involve(s) an individual or entity in any country of proliferation concern.

(c) The transaction reflect(s) a link between representatives of companies (e.g. same owners or management) exchanging goods, to evade scrutiny of the goods exchanged.

(d) The transaction(s) involve(s) the shipment of goods inconsistent with normal geographic trade patterns, i.e. where the country involved does not normally export or import the types of goods concerned, or the vessel is listed in the UN sanctions lists.

(e) Companies or individuals from countries, other than the country of the stated end-user, place the order for goods.

11.3 Jurisdiction:

(a) Countries with weak financial safeguards and which are actively engaged with a sanctioned country.

(b) The presence of an industry that produces dual-use goods, proliferation-sensitive items or military goods.

(c) Deliberate insertion of extra links into the supply chain.

(d) Countries that are known to have weak import/export control laws or poor enforcement.

(e) Countries that do not have the required level of technical competence concerning certain goods involved.

11.4 Other:

(a) The final destination or end-user is unclear.

(b) Project financing and complex loans, where there is a presence of other objective factors such as an unidentified end-user.

(c) Declared value of shipment under-valued in relation to shipping cost.

(d) Inconsistencies in information contained in trade documents and financial flow e.g. names, addresses, final destination.

(e) The use of fraudulent documents and identities e.g. false end-use certificates and forged export certificates.

(f) The use of facilitators to ensure the transfer of goods avoids inspection.

(g) A freight forwarding company being listed as the product's final destination.

(h) Wire instructions or payment from or due to entities not identified on the original letter of credit or other documentation.

(i) Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.

CONCLUSION

It is expected henceforth that NBFIs will follow, at a minimum these guidance notes and will apply enhanced due diligence when dealing with countries on the UN or EU sanctions lists, or residents of those countries, or transactions associated with those countries (see EU Sanctions Risk List Countries). NBFIs

are expected to enhance their risk management programme to ensure that they are not engaging people or entities that are appreciably exposed to proliferation risk, rather than attempting to manage those risks.

Any NBFIs operating internationally, or possessing international clients, who choose to do business with countries with a high risk profile, will need to know in real time which countries are on the EU or UN sanctions lists, as per the UK/EU Specially Targeted List or as per the OFAC listing, and carefully monitor any connections to those countries, including reporting suspicious transactions to the Financial Intelligence Agency in a timely manner.

NBFIs should be sensitive to the risks associated with financing the potential tools of proliferation, including nuclear and dual use material, and military items.

*** END ***